REMARKS

Applicant requests favorable reconsideration of the subject application in view of the preceding amendments and the following remarks.

Claims 1-20 are pending in the application with Claims 1, 15 and 18 being independent. Claim 1 has been amended herein, to clarify features of the invention. No new matter has been added.

Rejection of Claims 1-14

Claim 1 stands rejected under 35 USC 103(a) as being unpatentable over Wasilewski (U.S. Patent 6,424,714) in view of Hendricks (U.S. Patent 5,600,364) and further in view of Xiao (U.S. Patent No. 6,571,337). Applicant requests reconsideration and removal of this rejection for at least the following reasons.

To establish a prima facie case of obviousness, all of the recited claim limitations must be taught or suggested in the prior art (See MPEP §2143.03). Applicant submits the combined teachings of the cited references, as applied in the Office Action, fail to teach each of the limitations recited in present Claim 1; and hence, fail to render Claim 1 unpatentable as a matter of law.

As an initial matter, Applicant submits the Office Action fails to present a *prima facie* case of obviousness, as it fails to reference valid portions of Wasilewski as supporting the present rejections. For example, the Office action refers to "column 30 lines 32-47" and "column 30 lines 48-67" as supporting the present rejections. *See, e.g., 11/23/2005 Office Action, page 2.* However, the referenced Wasilewski has only 28 columns. Accordingly, Applicant requests reconsideration and removal of the present rejections, or in the alternative, at least a new, non-final Office action that correctly identifies those portions of Wasilewski upon which the Examiner actually relies upon as supporting the present rejections, so that Applicant may be afforded a reasonable opportunity to respond on the merits.

The above notwithstanding, Applicant will in any event address the present rejections as they are best understood. The Examiner argues Wasilewski discloses a system that provides conditional access to services, wherein the user can select an event, and the agent responds by sending an EMM containing the necessary entitlement information. *See, 11/23/2005 Office Action, page 2.* A detailed review of Wasilewski, however, fails to reveal even a single reference to any "agent".

While Wasilewski may generally disclose that a customer 130 may select programs from a menu, *see, col. 5, lines 53-55*, and that a signed, encrypted EMM is transferred to an STU 90 via a digital network 70, *see, col. 11, lines 57-59*, each of the recited limitations of Claim 1 is not taught or suggested. Moreover, the secondary references of Hendricks and Xiao do nothing to remedy the deficiencies of Wasilewski.

In contradistinction to the cited references of record, independent Claim 1 recites:

> A method for managing access to a scrambled event of a service provider, said method comprising:
>
> receiving in a device an electronic list of events, at least one event having a digitally signed encrypted message associated therewith, said encrypted message comprising a descrambling key and event information including at least one of a channel identity, date and time stamp, event identity and payment amount corresponding to said associated event;
>
> receiving in said device, in response to user selection of said event, said digitally signed encrypted message;
>
> authenticating in said device, a source of the digitally signed encrypted message in response to said digitally signed encrypted message;
>
> decrypting in said device, said digitally signed encrypted message to obtain said descrambling key upon said authenticating;
>
> receiving in said device, said selected event from the service provider, said selected event being scrambled using said descrambling key for preventing unauthorized access to said selected event; and
>
> descrambling in said device, said selected event using said descrambling key.

Claim 1 thus calls for receiving in a device, in response to user selection of an event, a digitally signed encrypted message comprising a descrambling key and event information, receiving, in the device, the selected event from the service provider, the selected event being scrambled using the descrambling key, and descrambling, in the device, the selected event using said descrambling key. Wasilewski's EMM delivery fails to meet any of these limitations. Rather, the EMM of Wasilewski merely contains an encrypted MSK. *See, e.g., col. 11, lines 43-59 ("a clear EMM carr[ies] the MSK and a token.").* Furthermore, the Wasilewski MSK is not a descrambling key used to descramble a delivered event. Rather, the MSK is what is referred to by Wasilewski as a "second level encryption key". *See, e.g., col. 8, lines 12-15.* This second level encryption key encrypts the control words, which are actually used to encrypt the program bearing MPEG-2 transport packets. *See, e.g., col. 8, lines 9-12.*

Wasilewski's purported agent sending an EMM containing entitlement information fails to teach or suggest a digitally signed encrypted message comprising a descrambling key and event information as recited in Claim 1. The Examiner acknowledges this deficiency of Wasilewski and submits that "Wasilewski does not disclose an encrypted message comprising [a] descrambling key and authenticating a source of digitally signed encrypted message in response to said digitally signed encrypted message and obtaining the descrambling key upon said authenticating." *See 11/23/2005 Office Action, page 3.* The Examiner attempts to remedy these admitted shortcomings of Wasilewski by incorporating select portions of Xiao.

More particularly, the Examiner argues Xiao teaches an encrypted message comprising a descrambling key and a description of the content in col. 4, lines 17-33 (*See 11/23/2005 Office Action, page 3),* and, that Xiao authenticates the message and obtains a descrambling key upon the authenticating. *See 11/23/2005 Office Action, pgs. 3-4.* However, a detailed reading of Xiao reveals Xiao does not teach or suggest receiving a digitally signed encrypted message, authenticating a source of the digitally signed encrypted messages, decrypting the digitally signed encrypted message, receiving the selected event and descrambling the selected event in a same device distinct from the service provider – as is recited in amended Claim 1.

As described in col. 4, line 43 - col. 5, line 34, Xiao first transmits an information entity that contains the encrypted content encryption key, encrypted by the public key of the publisher's clearance center; a delayed retrieval description; and a URL that locates the publisher's content server to a user. The delayed retrieval description provides information regarding where the data entity is stored in the publisher's store, and which program is to be used to handle retrieval of the data entity. If the user is interested in obtaining the data entity associated with the information entity, a request is issued by the user. A content server authenticates the request, decrypts the content key and uses the information entity's delayed retrieval description to retrieve the requested data entity. The content server then sends the unlocked content key to the user. *See, col. 5, lines 54-58.*

Thus, Xiao, like Wasilewski, fails to teach receiving a digitally signed encrypted message, authenticating a source of the digitally signed encrypted message, decrypting the digitally signed encrypted message, receiving the selected event and descrambling the selected event in a same device distinct form the service provider, as is recited in amended Claim 1.

As the Examiner relies upon Hendriks solely for its purported teachings regarding event information comprising a channel identification, it also fails to remedy the shortcomings of the above-cited references.

Further, Wasilewski actually teaches away from such a configuration, as it expressly teaches a three (3) level encryption scheme that encrypts code words using MSKs. In contrast, Xiao merely teaches two (2) levels of security. *See, e.g., col. 4, lines 22-24.* Accordingly, Applicant submits a proper motivation for replacing the three (3) level protection scheme of Wasilewski with the two (2) level encryption scheme of Xiao is lacking, as it would assumedly lessen the amount of security provided by Wasilewski.

Accordingly, Applicant respectfully traverses the rejection of Claim 1, and requests its reconsideration and removal, as the cited art fails to teach or suggest each and every limitation present in Claim 1. Applicant also requests reconsideration and removal of the rejections of Claims 2-14 as well, at least by virtue of these claims' ultimate dependency upon a patentably distinct base Claim 1.

Rejection of Claims 15-20

Claims 15 and 18 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Wasilewski in view of Pinder (U.S. Patent No. 5,742,677). Applicant traverses these rejections, and requests their reconsideration and removal.

As part of the present rejection, the Examiner again refers to "column 30 lines 32-47" and "column 30 lines 48-67" of Wasilewski as supporting the present rejections. *See, e.g., 11/23/2005 Office action, page 2.* However, as discussed previously, Wasilewski has only 28 columns. Further, while Claims 15 and 18 stand rejected as being unpatentable over Wasilewski in view of Pinder, the Office Action makes reference to the teachings of Nagel and Xiao. The purported teachings of Nagel and/or Xiao do not support the rejections of Claims 15 and 18 over Wasilewski in view of Pinder. Accordingly, Applicant requests reconsideration and removal of the rejections, or in the alternative, at least a new, non-final Office Action that correctly references those prior art references, and portions of those prior art references, upon which the Examiner actually relies upon as supporting the present rejections – so Applicant may be afforded a reasonable opportunity to respond thereto.

The above notwithstanding, Applicant requests reconsideration and removal of the rejections of Claims 15 and 18 for reasons analogous to those set forth with regard to Claim 1. Claims 15 and 18 are both directed to methods for managing access between a device having a smart card coupled thereto and a service provider, <u>said device performing the steps of</u> "authenticating said guide provider". The Examiner admits that Wasilewski fails to teach this limitation. Moreover, the secondary reference Xiao fails to remedy the acknowledged deficiency of Wasilewski. For example, line 22 of col. 5 of Xiao expressly teaches authentication is performed by the content server – and not the user device as is recited by Claim 15. *See, e.g., col. 5 line 22 ("[t]he content server authenticates ... ").* As Pinder is relied upon merely for its purported teachings regarding use of a private key for a digital signature, Pinder also fails to remedy the shortcomings of Wasilewski and Xiao in this regard. Applicant is unsure of how the Examiner is intending to apply the Nagel reference. *(See 11/23/2005 Office Action, page 5, para. 3).*

In view of the foregoing, the rejections of Claims 15 and 18 are traversed. Reconsideration and removal of these rejections are requested. Applicant also requests reconsideration and removal of the rejections of Claims 16, 17, 19, and 20, at least by virtue of these claims' ultimate dependency upon a patentably distinct base Claim 15 or 18.

Having fully addressed the Examiner's rejections it is believed that, in view of the preceding amendments and remarks, Claims 1-20 of this application stand in condition for allowance. Accordingly reconsideration and an early notice of allowance are respectfully solicited.

If necessary, Applicant's representative may be reached by telephone at 585-232-6500.

Respectfully submitted,

Dated: April 24, 2006

Michael J. Didas, Registration No. 55,112
HARTER, SECREST & EMERY LLP
1600 Bausch & Lomb Place
Rochester, New York 14604
Telephone: 585-232-6500
Fax: 585-232-2152